Claims

What is claimed is:

1.   A method for a probing entity to detect a duplicate IP address, the method comprising:

generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact;

waiting a random period of time related to the identifying value;

sending one or more first ARP probes onto the network with which the probing entity desires to interact;

determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict;

determining whether the probing entity is connected to an active network;

sending one or more second ARP probes onto the network with which the probing entity desires to interact; and

determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict.

2.   The method of claim 1, comprising:

sending ARP probes until the probing entity is connected to an active network.

3.   The method of claim 2, comprising:

not employing the potentially duplicate IP address until after all the processing associated with claims 1 and 2 has been completed.

4.   The method of claim 1, wherein the length of the random period of time is generated by examining at least one of a GUID, a physical address, an IP address and a counter.

5.   The method of claim 1, wherein the one or more first ARP probes contain the physical address of the probing entity and a potentially duplicate IP address.

6. The method of claim 5, wherein the response to the first ARP probes contain the physical address of the probing entity, the physical address of a responding entity, the IP address of a responding entity and the potentially duplicate IP address.

7. The method of claim 6, wherein determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict comprises comparing the potentially duplicate IP address of the response to the potentially duplicate IP address associated with the probing entity.

8. The method of claim 7, wherein the one or more second ARP probes contain the physical address of the probing entity and a potentially duplicate IP address.

9. The method of claim 8, wherein the response to the second ARP probes contain the physical address of the probing entity, the physical address of the responding entity, the IP address of the responding entity and the potentially duplicate IP address.

10. The method of claim 9, wherein determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict comprises comparing the potentially duplicate IP address of the response to the potentially duplicate IP address associated with the probing entity.

11. The method of claim 1, wherein determining whether a probing entity is connected to an active network comprises at least one of (1) analyzing network traffic received by a network interface associated with the probing entity, (2) analyzing electrical signals received from hardware associated with the network with which the probing entity desires to interact and (3) analyzing BPDUs (Bridge Protocol Data Units) received by a network device associated with the network with which the probing entity desires to interact.

31

12. A computer readable medium storing computer executable instructions operable to perform a method for a probing entity to detect a duplicate IP address, the method comprising:

generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact;

waiting a random period of time related to the identifying value;

sending one or more first ARP probes onto the network with which the probing entity desires to interact;

determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict;

determining whether the probing entity is connected to an active network;

sending one or more second ARP probes onto the network with which the probing entity desires to interact; and

determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict.

13. The computer readable medium of claim 12, where the method further comprises:

sending ARP probes until the probing entity is connected to an active network.

14. The computer readable medium of claim 13, where the method further comprises:

not employing the potentially duplicate IP address until after all the processing associated with claims 12 and 13 has been completed.

15. A system for detecting and preventing the use of duplicate IP addresses comprising:

a random time period generator operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator;

a probe generator operable to produce an ARP probe;

a response analyzer operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and

an active network detector operable to determine whether the system is connected to an active network.

16.   The system of claim 15, wherein the active network detector comprises at least one of: (1) a network traffic analyzer operable to analyze network traffic and to determine whether the probing entity is connected to an active network; (2) a network pulse analyzer operable to analyze one or more electrical signals received from network devices operably connected to the probing entity and to determine whether the probing entity is connected to an active network, and (3) a BPDU analyzer operable to analyze one or more bridge protocol data units received by network devices operably connected to the probing entity and to determine whether the probing entity is connected to an active network.

17.   A computer readable medium storing computer executable components of a system for detecting and preventing the use of duplicate IP addresses, the system comprising:

a random time period generating component operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator component;

a probe generating component operable to produce an ARP probe;

a response analyzing component operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and

an active network detecting component operable to determine whether the system is connected to an active network.

33

18.   A system for detecting and preventing the use of duplicate IP addresses comprising:

means for identifying a random period of time that should be waited before a probe generating means is activated;

means for generating an ARP probe;

means for distributing the ARP probe to one or more IP components;

means for interpreting a response to the ARP probe; and

means for determining whether a probing entity is connected to an active network.